2M

УДК 681.3

А.О. Мелащенко
Институт кибернетики им. В.М. Глушкова НАН Украины, г. Киев
javatask@ukr.net

Язык описания политик подписания. Схема и возможности

Описано предназначение и функциональное наполнение политик подписания. Представлена OWL-схема ее представления и показано использование политик подписания на примере государственных тендерных закупок.

Введение

Внедрение в Украине общественной структуры для поддержки электронной цифровой подписи (ЭЦП) требуют строгого описания и поддержания политик безопасности. Это связано с необходимостью повышения конкурентоспособности при использовании в eCommerce, eTransport и eGovernment, внутри страны и за ее пределами, что невозможно без гарантированного обеспечения уровня доверия и надежности таких систем. К тому же, вступление Украины в ВТО требует создания интеллектуальных систем, способных анализировать, сравнивать и выполнять разновидности политик безопасности согласно требованиям обеспечения транзакций в разных странах и бизнес-алгоритмах.

Один из недостатков текущих спецификаций и соответственно реализаций ЭЦП – отсутствие прямой связи семантики бизнес-алгоритмов с ЭЦП, поскольку семантика распознается косвенно, через контекст транзакции. Такой механизм недопустим в системах с повышенными требованиями к надежности и безопасности транзакций, например, государственных закупок, банковских транзакций и т.п.

Для привязки семантики к дополнительным правилам верификации и валидации ЭЦП разработана концепция политики подписания, предполагающая ее разновидности. Политики подписания – пока слаборазвитое поле, в первую очередь ввиду нечеткости границ их использования и недостатка опыта стандартизации. А механизм описания политик подписания – критически важный инструмент для поддержки валидации ЭЦП на этапе подписания и привязки четкой семантической нагрузки ЭЦП.

В этой статье рассмотрены требования к политике подписания, в частности ее функционального наполнения. Предложен расширяемый механизм описания политик подписания, который в частности допускает организацию автоматического сравнения политик подписания.

1. Определение поля использования политик подписания

Для определения контекста и функционального наполнения политик подписания рассмотрим определение политики безопасности для общественной структуры поддержания ЭЦП. Политика безопасности – документ, декларирующий, как компания

планирует защитить свои физические и информационно-технологические активы. Как «живой документ», политика безопасности означает, что формирование документа перманентно не завершается, он непрерывно обновляется по требованиям технологий и обслуживающего персонала.

Согласно Директиве [1], общественную структуру в поддержку ЭЦП составляют множества субъектов и объектов, каждый из которых имеет свои политики безопасности, которые включают, например, требования к политикам сертификации для провайдеров, выдающих усиленные сертификаты [2], требования к политикам органов штемпелевания времени [3] и т.п. Одна из составляющих политики безопасности – политика подписания, которая согласно «Отчету о политиках подписания» [4] есть набор правил для создания и валидации ЭЦП, используя который ЭЦП можно определить как валидную. Поскольку политика – общий способ выразить функциональные условия электронного бизнеса, политику подписания нужно отличать от другой составляющей политики безопасности – политики сертификации, содержащей правила, которые *среди прочего* определяют, какая политика сертификации приемлема под конкретной политикой подписания. Это ограничивает сертификаты открытых ключей, используемые под политикой подписания, поскольку эти сертификаты должны содержать информацию (например, OID), указывающую, что они выполняют «такую» политику сертификации.

Далее определим, (1) контекст использования политики подписания, (2) ее контент или функциональное наполнение, (3) поле использования.

1.1. Контекст использования

1.1.1. Контекст транзакции. Поскольку политика подписания может задавать требования, ассоциированные с транзакциями, необходимо связать ее со специфическими базовыми элементами политики подписания, предназначенными для такой формализации. Контекст транзакции может включать коммерческий, административный, частные аспекты или их комбинацию. Контекст транзакции определяет общие приемлемые правила, ассоциированные с процедурами подписания. Такие правила могут произойти из состояний, например, действие должно быть предпринято при заполнении определенной формы согласно корпоративным условиям.

Например, центры сертификации ключей в Украине продают клиентам ЭЦП, ассоциированные с разным уровнем криптозащиты и, разумеется, с разной стоимостью: электронная печать компании, ЭЦП главного менеджера компании, бухгалтера и других служащих. Разумеется, виды электронных документов, исходящих из компании, следует подписывать разными ЭЦП согласно строгим процедурам организации электронного документооборота как основы политик подписания.

1.1.2. Политика подписания в пределах PKI. В среде PKI, когда подписант в цифровой форме подписывает данные, необходимо указать, что ЭЦП имеет определенное значение. ЭЦП может подтолкнуть подписанта к действию, связанному с выраженной фиксацией транзакции, или просто использовать как вызов, когда необходима аутентификация. Когда у ЭЦП есть определенное значение, подписант обязан включить индикацию этого в подписанную структуру о том, что ЭЦП – фиксация транзакции.

Как индикация политика подписания обеспечивает нотацию относительно преобладающих правил и условий, которые подписант формулирует для третьих лиц, включая зависимые стороны, которые полагаются на его ЭЦП.

1.2. Контент политики подписания

Политика подписания определяет технические и процедурные требования относительно создания подписи и ее валидации для соответствия определенным бизнес-потребностям. Политика подписания должна существовать в двух формах:

– понятных всем пользователям;

– обрабатываемых компьютером, возможно, внутренних встроенных кодах или внешних кодах, интерпретируемых компьютером.

Автоматизированную валидацию ЭЦП можно использовать в транзакциях, основанных на EDI-форматах электронного обмена данными (Electronic Data Interchange). EDI-транзакции включают транзакции таких финансовых услуг, как передача электронных фондов (EFT – Electronic Fund Transfer), обычно основанных на стандартах UN/EDIFACT [5]. Более новый формат для обмена структурированными данными основан на XML, в частности ebXML [6] как формат данных для обмена документа во всемирной паутине (WWW).

Согласно [4] общая информация о политике подписания включает:

1. Имя издателя политики подписания (A Signature Policy Issuer name).
2. Идентификатор политики подписания (A Signature Policy Identifier).
3. Период подписания (A Signing period).
4. Дата издания (A Date of issue).
5. Поле применения (A Field of Application).

Определенные фиксации (commit) транзакции, которые могут предпринимать участники транзакции, могут также составлять часть политики подписания. Такие фиксации транзакции устанавливают транзакционную структуру для использования цифровых подписей, подписывая документ. Тип фиксации транзакции может быть объектным идентификатором с квалификатором, обеспечивающим подробную информацию о фиксации транзакции, например, информацию о договорном/юридическом/прикладном контексте.

1.2.1. Информация о валидации ЭЦП. Информацию о валидации ЭЦП можно включать в общие правила или в правила фиксации транзакции, но в любом случае они не должны вступать в противоречие. Издатель политики подписания должен будет выбрать информационные элементы валидации ЭЦП, приемлемые для данной политики валидации ЭЦП. Информационные элементы валидации ЭЦП включают:

1) правила для использования органами сертификации (то есть требования построения пути сертификатов);

2) правила, относящиеся к пользовательскому сертификату;

3) правила удостоверения, что ЭЦП создана в то время, когда сертификат был валиден (то есть верхний предел времени валидности ЭЦП либо наличие временного штемпеля или метки времени);

4) правила для предостерегающего периода;

5) правила для использования информации о состоянии аннулирования (то есть требования аннулирования);

6) правила для защиты от компрометации ключа органа сертификации и слабой криптографии;

7) правила, касающиеся среды, которую будет использовать подписант;

8) данные верификации подписи, которые будут предоставлены подписанту или собраны верификатором;

9) любые ограничения на алгоритмы подписания и длину ключа;

10) правила для использования ролей субъектов политики безопасности;
11) требования построения пути сертификатов.

Требования сертификации идентифицируют последовательность надежных привязок, используемых для запуска (окончания) обработки пути сертификатов и начальные условия для его валидации, как определено в IETF RFC 2459 [7]. Детальная информация в «Отчете о политиках подписания» [4].

2. Язык описания политики подписания

В [8] представлена общая XML-разметка для ссылки на политики подписания в рамках стандарта XML-формата ЭЦП [9], но непосредственно отсутствует разметка для описания политик подписания. Для создания языка описания политик подписания рекомендуется глубоко исследовать и при необходимости разработать стандарты [10], [11]. В этой статье изучены новые версии этих стандартов [12], [13].

2.1. P3P

Платформа для проекта приватных предпочтений (P3P) позволяет веб-сайтам выразить свои приватные предпочтения в стандартном формате, может быть извлечена автоматически и легко интерпретироваться пользовательскими агентами. Именно они информируют пользователей о методах сайта (в машино- и человеко-читаемых формах) и автоматизируют принятие решений, основанное на этих методах. Таким образом, пользователи не должны учитывать политику конфиденциальности на каждом сайте, который они посещают.

Хотя P3P гарантирует, что пользователям будет сообщено о политике конфиденциальности прежде, чем они передадут личную информацию, P3P не обеспечивает механизм для удостоверения, что сайт функционирует согласно своей политике. P3P-продукты могут способствовать этому, но это – специфика реализации. Однако P3P является дополнением к законам и саморегулируемым программам, способным обеспечить механизмы, которые выполнят это требование. Кроме того, P3P не имеет механизмов передачи данных или поддержки безопасности при передаче или хранении персональных данных. P3P можно встроить в инструменты, облегчающие передачу данных и обеспечивающие соответствующие гарантии защиты информации.

Реализуя специфические требования для выражения политик конфиденциальности, P3P имеет более слабый механизм расширения и уступает RDF, что явно демонстрирует наличие RDF-разметки для P3P-политик конфиденциальности [15]. Механизм расширения критичен для политик безопасности, поскольку они являются «живыми документами», постоянно изменяемыми и расширяемыми.

2.2. RDF

Разработка «RDF/XML Syntax Specification (Revised)» наиболее перспективна с позиций гибкости механизмов. Согласно [14] структура для описания ресурсов (RDF – Resource Description Framework) является языком представления информации о ресурсах в WWW. Он предназначен для представления метаданных о таких ресурсах сети, как имя, автор и дата модификации веб-сайта, авторского права и лицензионную информацию о документе сети или списке доступности для некоторого общего

ресурса. Обобщив понятие ресурса сети, RDF можно использовать для представления данных о сущностях, идентифицируемых в сети, даже когда их невозможно непосредственно восстановить из сети.

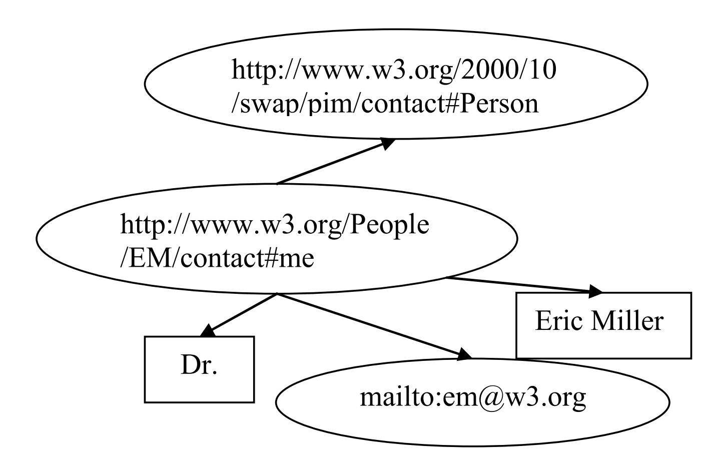


Рисунок 1 – Пример схемы описания контакта с человеком

RDF предназначен для ситуаций, в которых эту информацию обрабатывает приложение. RDF служит общей основой для выражения этих данных, поэтому ими могут обменяться приложения без потери значений. Поскольку это – общая структура, разработчики могут усилить пригодность общих анализаторов RDF и инструментов обработки.

RDF основан на идее идентификации сущности с использованием идентификаторов сети URIs (унифицированных идентификаторов ресурса) и описанием ресурса в терминах простых свойств и значений свойств. Это позволяет RDF представить простые утверждения о ресурсах как граф узлов и дуг, представляющих ресурсы, их свойства и значения. Для примера на рис. 1 приведен RDF-граф для утверждения «есть человек, идентифицированный http://www.w3.org/People/EM/contact#me, чье имя – Эрик Miller, чей адрес электронной почты – em@w3.org, и чья приставка – д-р».

Гибкость и простота механизмов RDF способствуют спецификации политик подписания. Это обусловлено механизмом свойств, типизацией и использованием URI. Далее детально о каждом свойстве.

1. RDF описывает ресурс в понятиях свойств.

2. RDF не имеет своих внутренних типов, а использует внешние определения, как правило, стандартные для XML [16]. Пример типизированного свойства «1999-08-16»^^xsd:date, где xsd – схема http://www.w3.org/TR/xmlschema-2/.

3. Как HTML, RDF/XML – машино-обрабатываемый и, используя URI, может связать информацию через сеть. Однако в отличие от обычного гипертекста RDF URI может обратиться к любой опознаваемой сущности, включая сущности, непосредственно не извлекаемые из сети (скажем, человек Эрик Miller).

Привлекательное свойство модели RDF – организация привязки свойств к объектам. В отличие от традиционной для программирования объектной модели, когда класс содержит свойства, свойства существуют в рамках класса, а заполнение свойств обязательно, в модели RDF классы привязывают к свойствам, то есть одно свойство может быть элементом множества или несвязанных между собой классов, а заполнять свойства необязательно.

Модели RDF имеют существенные недостатки, препятствующие ее использованию для описания политик подписания:

1) ограничения мощности на свойства, например, у человека есть точно один биологический отец;

2) определение, что данное свойство (скажем, ex:hasAncestor) является транзитивным, например если A ex:hasAncestor B и B ex:hasAncestor C, то A ex:hasAncestor C;

3) определение, что данное свойство – уникальный идентификатор (или ключ) для случаев специфического класса;

4) определение, что два разных класса (имеющих разные URIrefs) фактически представляют один класс;

5) определение, что два различных экземпляра класса (имеющих разные URIrefs) фактически представляют одни экземпляр класса;

6) определения ограничений на диапазон или мощность свойств, зависящих от класса ресурса, к которому применено свойство, например, для футбольной команды свойство ex:hasPlayers имеет 11 значений, а для баскетбольной – только 5 значений;

7) способность описать новые классы в терминах комбинаций (например, объединения и пересечения) других классов или сказать, что два класса являются разбиением (то есть не существует экземпляра, который одновременно является экземпляром обоих классов).

Развитие разметки RDF, именуемой OWL [17], снимает эти ограничения.

2.3. OWL

Язык OWL обеспечивает три выразительных диалекта, разработанных для использования определенными сообществами архитекторов и пользователей.

OWL Lite поддерживает пользователей, прежде всего нуждающихся в иерархической классификации и простом ограничении свойств. Например, хотя OWL Lite ограничивает мощность, он допускает только значения мощности 0 или 1. Более простым должен быть инструмент поддерживающего OWL Lite, чем его более выразительных родственников, чтобы обеспечить быстрый переход для тезаурусов и других таксономий [17].

OWL – модель и схема, в которой спецификация политик подписания будет наиболее полной и строгой, что критически важно для бизнес-транзакций.

Одновременно модель OWL дает возможность ужесточить требования и перевести язык описания в область экспертных систем, то есть в OWL DL. Даже без перехода в OWL DL можно сравнить политики подписания, используя конструкты группы (In)Equality, которые обеспечивают сравнение классов и свойств, реализацию инверсии и транзитивности.

Используя синтаксис OWL, определим схему для описания политик подписания, в которой реализованные атрибуты, идентифицированные в 1.2. Сама схема приведена в разделе 3, а пример применения – в разделе 4.

3. OWL-схема описания политик подписания

Исходя из определения политики подписания, ее составляющие представлены на рис. 2. Здесь SignaturePolicy как политика подписания состоит из:

– Базовых свойств (Core Properties) – специфицирует базовые свойства, без которых невозможна публикация политики подписания. Более детальное описание свойств 1.2.

– Базовых правил (Core Rules) – специфицирует базовые критерии, выполнение которых гарантирует валидность подписи.
– Правил уровня транзакции (Transaction Context Rules) – специфицирует базовые критерии, выполнение которых идентифицирует фиксацию транзакции.

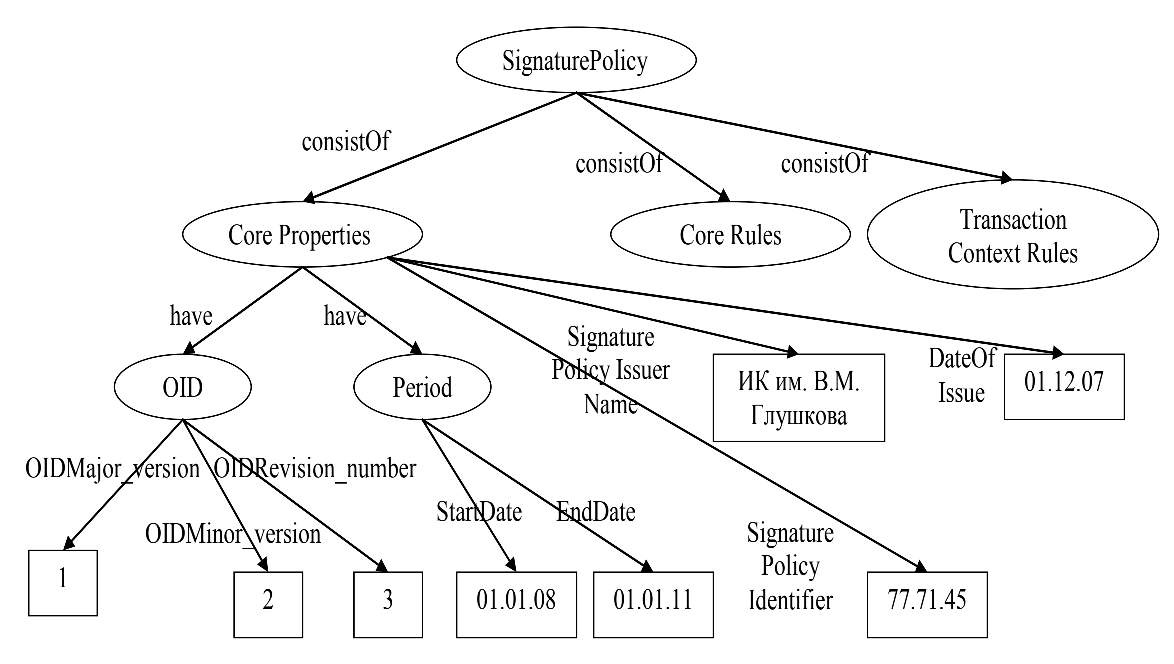


Рисунок 2 – Базовые элементы политик подписания

Конкретная спецификация базовых правил и правил уровня транзакции зависит от контекста использования политики подписания. Полноценное использование политики подписания, с полной спецификацией всех основных составляющих, продемонстрировано далее на конкретном примере.

4. Пример использования политики подписания

Рассмотрим процедуру приглашения для участия в государственных тендерных закупках. Отметим, что это одно из множества применений политики подписания.

Этот сценарий актуален сегодня в Украине, вступившей в ВТО, а предложенное применение можно распространить на предприятия любого размера, причем унификация процесса тендерных закупок снизит стоимость программного обеспечения и оптимизирует затраты предприятий и государства в целом.

Рассматривая государственные закупки, задействуем законопроект «Про закупку товаров, работ и услуг за государственные средства» [19]. В частности в параграфе 2 статьи 13 указано: «Замовник має право здійснити закупівлю за однією з процедур, зазначених у частині першій цієї статті (крім процедур торгів з обмеженою участю та закупівлі у одного учасника), шляхом здійснення електронних закупівель з використанням інформаційної системи в Інтернет з дотриманням вимог, установлених цим Законом та іншими актами законодавства України».

В рамках концепции базовых компонентов [20] UN/CEFACT разработал бизнес-модель и XML-форматы обменных документов для организации тендерных закупок, соответствующие требованиям ВТО. Этот проект eTendering разрабатывает комитет TBG6 UN/CEFACT [21].

Стандартизированные бизнес-процессы и документы обеспечат максимальную интероперабельность систем и прозрачность процессов. Использование наработок UN/CEFACT целесообразно и желательно в связи с положениями законопроекта, в частности с предназначением, указанным в пояснительной записке [22]: «Метою прийняття законопроекту є встановлення правових та економічних засад здійснення процедур державних закупівель для забезпечення реального дотримання сучасних принципів державних закупівель та подальшої *гармонізації національного законодавства* щодо державних закупівель *з нормами аналогічного міжнародного законодавства, зокрема Євросоюзу та у межах вступу України до СОТ*».

Участвующие в приглашении стороны – это организатор, участник и гарант. Валидными являются ЭЦП, когда каждый участник выполнил требования:

1. Организатор своей ЭЦП гарантирует корректность своих реквизитов, подтверждая номер тендера и связанную с ним информацию.
2. Включенные в приглашения реквизиты и параметры участника также подписаны предварительно зарегистрированным участником, при этом в характеристике предприятия указаны сертификаты необходимой квалификации персонала и сертификаты предприятия (скажем, о качестве выпускаемой продукции), подписанные соответствующими органами.
3. Гарант указывает свои реквизиты и дополнительные данные, подтверждающие корректность реквизитов и достаточность финансовых средств, оцененных и подписанных независимым оценщиком, для обеспечения гарантий между участником и организатором тендера, если его выиграет участник.

Только при условии выполнения указанных требований валидна ЭЦП на приглашении. Для выполнения поставленной задачи необходимо:

1. Описать бизнес-процесс.
2. Описать политику подписания, согласно требованиям тендера.
3. Указать методы валидации подписи на основе политики подписания.



Рисунок 3 – Передача приглашения участнику организатором

Конкретная спецификация базовых правил и правил уровня транзакции зависит от контекста использования политики подписания и может выглядеть негативно для определения политики подписания. На самом деле это не так, в идеологии инфраструктуры ebXML UN/CEFACT разрабатывает библиотеки стандартных, базовых атрибутов любого документа eCommerce, eGovernment и eTransport. А eTendering полностью базируется на идеологии базовых библиотек, поэтому можно выработать общий механизм спецификации политик подписания.

Бизнес-процесс показан на рис. 2. Политики подписания согласно вышеуказанным требованиям выглядят как на рис. 4.

Построение такой иерархии основано на источниках информации, указанных в политике подписания и DOM-модели XML-документа приглашения (рис. 5 и рис. 6).

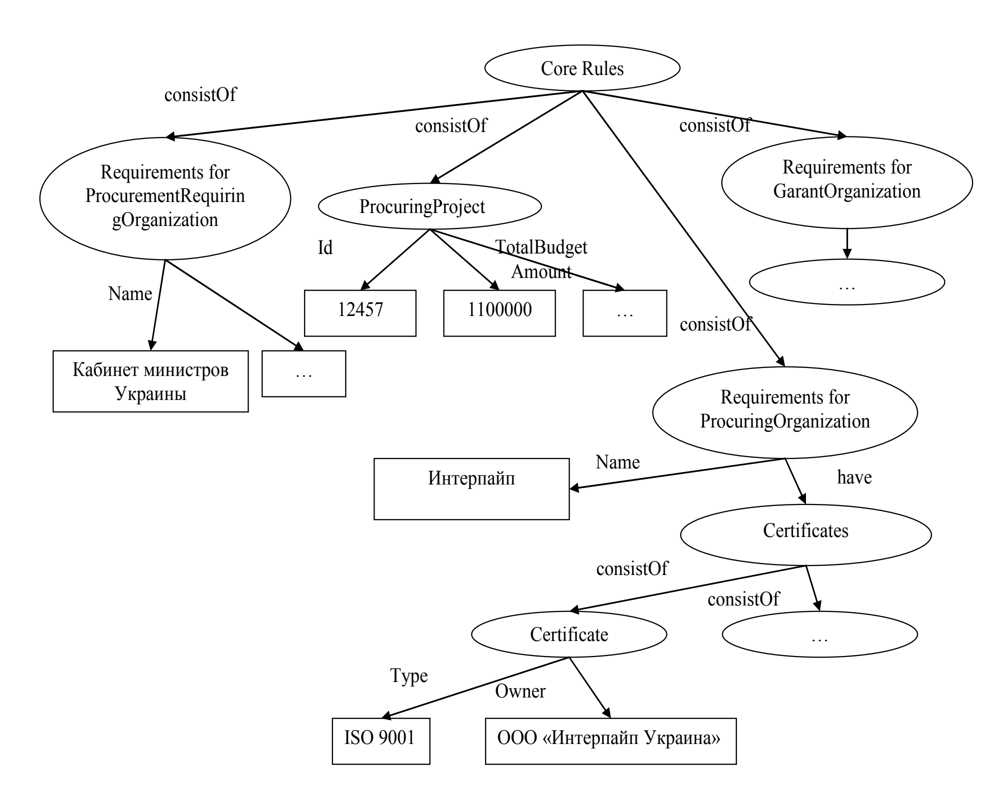


Рисунок 4 – Дополнительные правила валидации подписи

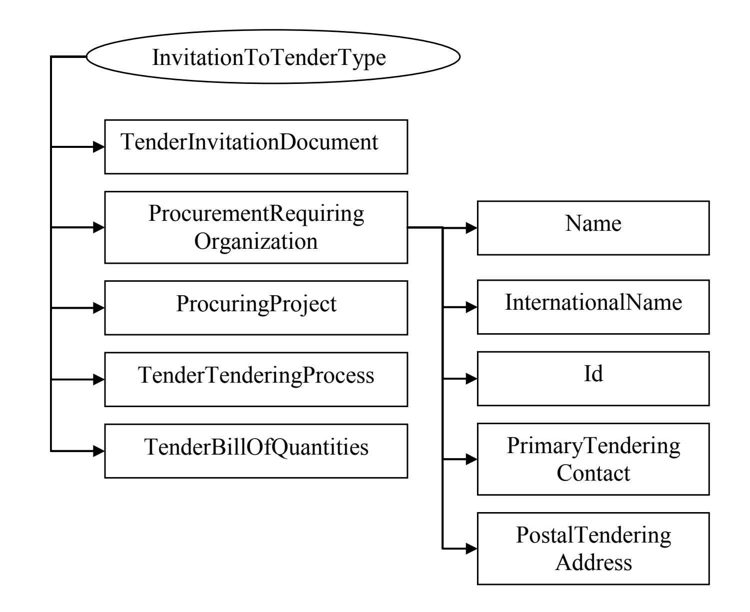


Рисунок 5 – Общая DOM-модель XML-документа, описывающая приглашение на тендер, и DOM-модель части XML-документа с атрибутами организатора

Источники данных, на основе которых заполняются множества допустимых значений политики подписания, таковы:

1. Реквизиты организатора – путь сертификации.
2. Номер и данные о тендере – сайт организатора тендера.
3. Реквизиты участника, к которым имеет прямой или косвенный доступ программа верификации данных.

4. Сертификаты о квалификации персонала для участника и наличие средств для гаранта – сайты соответствующих органов сертификации.

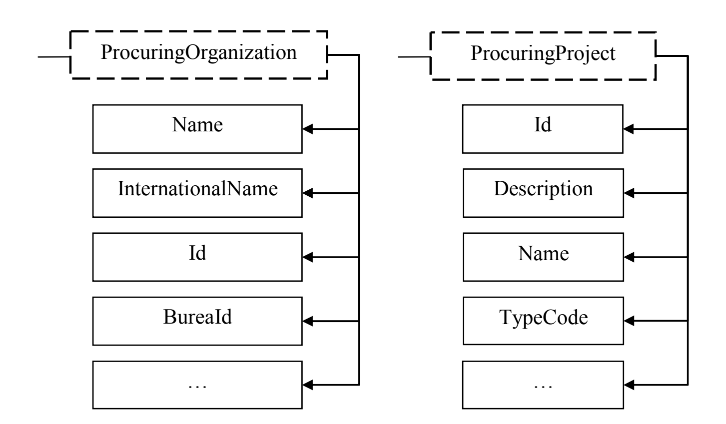


Рисунок 6 – DOM-модель части XML-документа, описывающая атрибуты участника, и DOM-модель части XML-документа, описывающая атрибуты тендера

Язык OWL позволяет задать DOM-модель политики подписания и определить пространство значений конкретных экземпляров документов и их полей. Используя политику подписания, для валидации документа необходимо сравнить конкретные элементы (поля) в DOM-модели документа, согласно которой политика подписания характеризуется множеством возможных значений любого экземпляра документа. Наращивание функционала происходит добавлением вершин в графовую DOM-модель, согласно политике подписания и документу соответственно. Определения уникальных идентификаторов, функциональных зависимостей и транзитивности языка OWL позволяют модифицировать DOM-модель политики подписания для более глубоких сравнений и спецификаций. Ввиду использования языка OWL, спецификация политики подписания гарантирует вычислимость выражений OWL и обработки их интеллектуальными агентами, преследующими цели, поставленные пользователем.

Таким образом, проанализировав содержание DOM-модели XML-документа приглашения на наличие допустимых значений всех атрибутов, можно установить валидность подписи на приглашении.

Выводы

Политики подписания – это составляющие политик безопасности в общественной структуре для поддержки электронных подписей. Политика подписания как механизм позволяет связать семантику с ЭЦП, таким образом, повышая доверие и надежность для eCommerce.

Нынче отсутствуют стандарты и даже специализированные разработки для предоставления политики подписания, ввиду сложности данных, непосредственно включенных в политику подписания, а также самой «живой» природы политики, то есть постоянно изменяющейся под потребности технологий и обслуживающего персонала.

В статье идентифицирован основной контент политики подписания и исследованы языки разметки для представления разнообразных данных в целях политики подписания. На примере организации тендерных закупок по правилам ВТО показана адаптация языка разметки OWL, идеально подходящего для предоставления «живой информации» и имеющего встроенные средства наращивания семантического богат-

ства и механизмов политик подписания. Использование человеко- и машино-читаемых политик подписания позволяет увеличить доверие и надежность eCommerce и достичь автоматического выполнения юридических и технических требований в разных странах и бизнесах.

Литература

1. Директива 1999/93/ЕС Европейского Парламента и Совета от 13 декабря, 1999 г. относительно структуры сообщества для электронных подписей.
2. ETSI TS 101 456 V1.4.3 (2007-05) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
3. ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
4. ETSI TR 102 041 V1.1.1 Signature Policies Report.
5. ДСТУ ISO 9735-1:2008 Обмін електронними даними для адміністрування, торгівлі і транспорту (EDIFACT) Правила синтаксису прикладного рівня (версія синтаксису номер 4, редакція синтаксису номер 1). Частина 1: Спільні для всіх частин правила синтаксису.
6. ISO/TS 15000-1:2004 Electronic business eXtensible Markup Language (ebXML). Part 1: Collaboration-protocol profile and agreement specification (ebCPP).
7. IETF RFC 2459: «Internet X.509 Public Key Infrastructure Certificate and CRL Profile».
8. ETSI TR 102 038 V1.1.1 TC Security – Electronic Signatures and Infrastructures (ESI); XML format for signature policies.
9. W3C 08-2001 (W3C/IETF Proposed Recommendation, August 2001): «XML-Signature Syntax and Processing».
10. W3C 2-1999 (W3C Recommendation, 22 February 1999): «Resource Description Framework (RDF) Model and Syntax Specification».
11. W3C 10-2000 (W3C Working Draft, 18 October 2000): «The Platform for Privacy Preferences 1.0 (P3P1.0) Specification».
12. W3C 2-2004 (W3C Recommendation 10 February 2004): «RDF/XML Syntax Specification (Revised)».
13. W3C 4-2002 (W3C Recommendation 16 April 2002): «The Platform for Privacy Preferences 1.0 (P3P1.0) Specification».
14. W3C 2-2004 (W3C Recommendation 10 February 2004): «RDF Primer».
15. W3C 1-2004 (W3C Note 25 January 2002): «An RDF Schema for P3P».
16. W3C 10-2004 (W3C Recommendation 28 October 2004): «XML Schema Part 2: Datatypes Second Edition».
17. W3C 2-2004 (W3C Recommendation 10 February 2004): «OWL Web Ontology Language Guide».
18. W3C 2-2004 (W3C Recommendation 10 February 2004): «OWL Web Ontology Language Semantics and Abstract Syntax».
19. Проект ЗУ «Про закупівлю товарів, робіт і послуг за державні кошти».
20. UN/CEFACT 11-2003 Core Components Technical Specification V2.01 «Core Components Technical Specification – Part 8 of the ebXML Framework».
21. Режим доступу: http://www.uncefactforum.org/TBG/TBG6/tbg6.htm.
22. Пояснювальна записка ЗУ «Про закупівлю товарів, робіт і послуг за державні кошти». – Режим доступу: http://gska2.rada.gov.ua:7777/pls/zweb_n/webproc4_1?id=&pf3511=31559.

А.О. Мелащенко

Мова опису політик підписання. Схема й можливості

Описано призначення й функціональне наповнення політики підписання. Наведено OWL-схему її подання й показано застосування політики підписання на прикладі державних тендерних закупівель.

A.O. Melashchenko

Description Language of the Signature Policy. The Scheme and Possibilities

The aim and functional filling of a signature policy is described. The OWL-scheme of its representation is presented and use of a signature policy on an example of the state tender purchases is shown.

Статья поступила в редакцию 18.07.2008.